

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR CRIMINAL COMPLAINT
AND ARREST WARRANT**

I, Jason Guyton, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to HSI Cleveland, Ohio. I have been so employed since March, 2009. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. I am an “investigative or law enforcement officer” of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

3. This affidavit is being submitted for the limited purpose of establishing probable cause that Craig A. GRUDEN, age 36, currently residing on High Tee Street, Willowick, Ohio, has received/distributed child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography).

4. The statements contained in this affidavit are based upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records. This affidavit includes only those facts

that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

RELEVANT STATUTES

5. This investigation concerns alleged violations of:
 - a. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), which prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit:
 - a. “Child Pornography,” as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
 - b. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1)

as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

- c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- d. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- e. “Peer to peer file sharing (P2P)” is a method of communication available to Internet users through the use of special publicly available software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s)

on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, conducting searches for files, or lists of files, that are currently being shared on another user's computer, and by viewing the files that another user has made available.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

7. On September 21, 2018, while performing undercover (UC) investigations on the mobile messaging application KIK, Royal Canadian Mounted Police (RCMP) Integrated Child Exploitation Group (BC ICE) Corporal Amanda Garner, using an undercover persona, joined a KIK chat group. Corporal Garner monitored the activity within this group and noted that the discussion of trading child pornography materials was prevalent among members. Corporal Garner observed users posting image and video files directly to the group message board. Additionally, members were posting URL links (at least 10 unique links) to the file sharing website "mega.nz" that directed users to image and video files depicting suspected child pornography. Lastly, users mentioned the file sharing website Dropbox and in at least one instant a user commented "Anyone have any links?". Between September 30, 2018, and October 3, 2018, Corporal Garner observed that the user "yummyxxxxyummyxxx" posted child pornography files in the group.

8. On October 12, 2018, Corporal Garner served a Production Order on KIK for the subscriber information and content/historical data for user "yummyxxxxyummyxxx". On November 21, 2018, KIK responded and it was determined that between September 24, 2018, and October 11, 2018, "yummyxxxxyummyxxx" received child pornography files directly from

other KIK users or within the group. In total, an additional thirty-four (34) KIK users were identified as being in possession of, and/or distributing image and video files depicting child pornography. One of those users was “**nowear5**”.

9. On December 12, 2018, BC ICE Constable Chantelle Foote served a Production Order on KIK for the subscriber information and content/historical data for all thirty-four (34) users to include “**nowear5**”. On January 31, 2019, KIK responded to the production order in full. The following subscriber details were provided by KIK for “**nowear5**”:

Username: nowear5
First name: No
Last name: Wear
Email: craig.gruden@att.net
User Locale: en
User Location: 98.27.208.143 – 2018/12/05
Client Info: country code=US
Registration: 2018/08/09 (Registration IP: 99.189.189.122)
Brand/Model: iPhone
Birthday: 1982-08-27

A query within the MaxMind IP Geolocation online database revealed that the IP address 99.189.189.122 geolocated in or near Eastlake, Ohio and is registered to the Internet Service Provider (ISP) AT&T U-verse.

10. Between January 31, 2019, and May 3, 2019, BC ICE reviewed and processed the results for all the users to include “**nowear5**”. BC ICE viewed the files provided by KIK and confirmed “**nowear5**” both sent and received files depicting child pornography. BC ICE further noted “**nowear5**” sent potentially self-identifying images which show they might have access to children.

11. In May 2019, HSI Cleveland received an investigative referral from HSI Vancouver

(British Columbia, Canada) regarding “**nowear5**”. On May 14, 2019, HSI Cleveland served a DHS Summons on AT&T, Inc. requesting subscriber information for IP address 99.189.189.122 on the following dates and times: 08/09/2018 at 03:34:88 hours until 12/04/2018 at 22:28:50 hours UTC. On May 20, 2019, AT&T provided the following subscriber information for the IP address:

| | |
|---------------------|--|
| Subscriber Name: | Craig Gruden |
| Subscriber Address: | 374 High Tee Street, Willowick, OH 44095 |
| Cell Phone: | (440) 478-6309 |
| Preferred Email: | craig.gruden@att.net |
| IP assigned: | 09/08/2017 – Current (Active) |

12. Your Affiant utilized a publicly available website to query the residents listed at 374 High Tee Street, Willowick, OH 444095 and discovered that the residents are listed as Craig GRUDEN and Nicole Gruden (nee Hannen).

13. On May 14, 2019, your Affiant conducted a computerized query of the Ohio Department of Public Safety database (OHLEG) which revealed the following: an Ohio Driver’s License issued to Craig A. GRUDEN, DOB: XX/XX/1982, SSN: XXX-XX-1694, 374 High Tee Street, Willowick, Ohio.

14. On May 23, 2019, HSI Cleveland received a DVD from BC ICE containing the evidence they collected for KIK user “**nowear5**”. KIK provided a total of 341 image and video files that were associated with the “**nowear5**” KIK account. Your Affiant reviewed all these files and found that many of them depict suspected child pornography. Your Affiant further observed that between August 9, 2018, and December 1, 2018, “**nowear5**” posted multiple files to KIK groups as well as sent files directly to individual KIK users. Some of these files can be further described as follows:

a. “1a0da594” – this 12 second video file depicts a naked prepubescent female lying on her back while an adult male masturbates his erect penis over her stomach. The adult male ejaculates onto the child’s face, chest, and stomach, and she can be heard crying during the recording. This video was sent from IP address 99.189.189.122 on November 30, 2018, at 3:17.

b. “18d105f4” – this 22 second video file depicts an adult female wearing stockings leaning back on a bed with a naked toddler kneeling in front of her. The toddler’s entire hand and wrist are inserted in the adult female’s vagina. During the video the adult female grabs the child’s arm and pulls it further into her. The adult female can also be observed rubbing her genitals. This video was sent from IP address 99.189.189.122 on November 26, 2018, at 3:43.

c. “fbc1500a” – this image file depicts a naked early pubescent and a naked prepubescent female sitting on the floor with their legs spread exposing their genitals to the camera. Both children’s faces are visible in the image and they are looking into the camera. This image was posted from IP address 99.189.189.122 on October 11, 2018, at 2:41.

d. “f2e30855” – this 1 minute 56 second video file depicts a naked prepubescent female on a couch. Throughout the video it appears that the child is being directed from off camera. The child can be observed rubbing a sex toy against her genitals as well as inserting it into her vagina. The camera focuses directly on her genitals at various points during the video. This video was posted from IP address 99.189.189.122 on November 30, 2018, at 9:34.

15. Your Affiant also observed that “**nowear5**” sent potentially self-identifying files using their KIK account. Although these files do not show the individual’s face, they do show his naked penis and buttocks. The files also show evidence that children (toys, child’s furniture, potty stool) may reside in the home where the images were taken.

16. Your Affiant conducted research on social media regarding this investigation and found the Instagram account “mrsgruden” with the vanity name “Nikki”. This account is set to private, but the profile picture shows an adult male and female posing with two (2) female children who appear to be under age ten (10). The adult’s in the profile picture appear to match the Ohio driver’s license photos of Craig GRUDEN and Nicole Gruden. The account also

includes the following quote on the cover page: “@cgruden1982’s adventure partner, permanent roommate, wife, Rosalynd & Vivienne’s momma. Lupus Warrior. Cross stitch enthusiast. CLE”. The Instagram account “cgruden1982” lists a vanity name of “Craig Gruden”. The account is set to private and the profile picture has no readily identifiable characteristics.

17. On June 17, 2019, at approximately 17:30 hours your Affiant conducted surveillance at and around the 374 High Tee Street, Willowick, Oh 44095. Your Affiant observed a light-colored Ford sedan, bearing Ohio License Plate EYA4417 parked in the garage of the 374 High Tee Street, Willowick, OH 44095. The garage door was open, and the vehicle was visible from the road. A query of OHLEG shows this vehicle is currently registered to GRUDEN at the 374 High Tee Street, Willowick, Oh 44095. Your Affiant also observed a child’s outdoor playset in the backyard of the 374 High Tee Street, Willowick, Oh 44095.

SEARCH OF 374 HIGH TEE STREET, WILLOWICK, OH 44095

21. On July 16, 2019, a search warrant, authorized by United States Magistrate Judge William H. Baughman, Jr., was executed at 374 High Tee Street, Willowick, OH 44095. The warrant was executed without incident and items including laptop computers, desktop computers and cellphones were seized. Craig A. GRUDEN, his wife Nicole, and the couple’s two (w) minor children were present.

22. An on scene forensic examination of GRUDEN’S Apple iPhone revealed multiple image and video files of suspected child pornography. Your Affiant reviewed these files and found some of them matched files contained in the “**nowear5**” KIK account.

23. During an interview conducted by your Affiant, GRUDEN admitted to utilizing KIK and other social media platforms to send and receive files depicting suspected child

pornography. GRUDEN stated he used “nowear” for the username on some of these accounts. GRUDEN stated that he has email accounts on Gmail and AT&T, and that the addresses include the name “Craig Gruden”. GRUDEN admitted to using peer-to-peer files sharing programs in the past and stated he may have used it to find child pornography. GRUDEN admitted to engaging in this behavior for more than ten (10) years. GRUDEN stated that the child pornography on his iPhone would be found under the application “File Box”. GRUDEN further admitted that he might have child pornography files on his old desktop and laptop computers.


CONCLUSION

27. Based on the foregoing, there is probable cause to believe that Craig A. GRUDEN violated 18 U.S.C. § 2252A(a)(2)(A) (receiving and distributing child pornography).


S/A Jason M. Guyton
Homeland Security Investigations



Sworn to via telephone after
submission by reliable electronic
means. Crim.Rules. 4.1; 41(d)(3)


Thomas M. Parker
United States Magistrate Judge
1:51 PM, Jul 16, 2019